METHOD AND DEVICE FOR INTERMEDIATE STORAGE OF SUBSCRIBER DATA DURING A RELOCATION OF A MOBILE SUBSCRIBER WITHIN A MOBILE COMMUNICATION NETWORK

CLAIM FOR PRIORITY

5   This application is a national stage of PCT/EP2004/050613 which was published on November 18, 2004 and which claims the benefit of priority to German Application No. 103 19 982.9 filed May 5, 2003.

TECHNICAL FIELD OF THE INVENTION

10   The invention relates to a method and a device for intermediate storage of subscriber data during a relocation of a mobile subscriber within a mobile communication network.

BACKGROUND OF THE INVENTION

15   In the course of a relocation of a UMTS/GPRS mobile radio subscriber in some case the packet switch routing the traffic (SGSN = Serving GPRS Support Node) has to be changed. The extract from the Standard (3GPP TS 23.060) shown schematically in Figure 1 presents the situation
20   schematically.

Figure 1 shows the forwarding of subscriber data (user data routing), if the Serving Radio Network Controller (SRNC =) and the Target Radio Network Controller (TRNC =) are connected to different network nodes (SGSN =
25   Serving GPRS Support Node) which support the GPRS (General Packet Radio Service) before a relocation (SRNS = Serving Radio Network Subsystem Relocation) takes place. Figure 2 shows the forwarding of subscriber data after the procedure "SRNS Relocation" and when the
30   procedure "Routing Area Update" is ended. In the case

shown the mobile station (MS) is in the status "PMM-
CONNECTED".

Before the procedure "SRNS Relocation" and "Routing Area
Update" the mobile station is registered at the "old"
SGSN. The origin RNC operates as serving RNC. After the
procedures "SRNS Relocation" and "Routing Area Update"
(RA = Routing Area) - as indicated in Figure 2 - the
mobile station is registered at the "new" SGSN. The
mobile station is in the status "PMM-CONNECTED" in
relation to the new SGSN and the destination RNC operates
as serving RNC.

In this case there is a "hole", in which data is already
being transmitted over the new connection (Message 7 in
Figure 3), although the subscriber is not yet known
there. In itself this is no problem for the data
transmission and is of no significance, for Lawful
Interception (LI) however it produces a problem since it
can only be decided when the subscriber data has been
completely transmitted (message block 14 in Figure 3)
whether the subscriber is to be subject to surveillance
or not. However in previous methods data had already been
transmitted which is then lost for surveillance.

SUMMARY OF THE INVENTION

In one embodiment of the invention, there is a method for
intermediate storage of data packets during a relocation
of a mobile subscriber within a communication network,
with the data packets, once the data transmission path
has moved from a switching network node originally
responsible for the subscriber to a switching network
node which is to become responsible for the subscriber
are stored in the last switching network node until the
subscriber data provided for the new data transmission

path is located in the last switching network node.

In another embodiment, there is a network node suitable for intermediate storage of data packets during a relocation of a mobile subscriber within a communication
5   network featuring a device for intermediate storage of data packets after the data transmission path changes from a switching network node originally responsible for the subscriber to the the network node, until such time as the subscriber data provided for the new data
10   transmission path is available.

BREIF DESCRIPTION OF THE DRAWINGS

The invention is described below in more detail with reference to exemplary embodiments and the figures, in which:

15   Figure 1 shows a network layout for routing subscriber data.

Figure 2 shows a network arrangement after the end of the relocation procedure.

Figure 3 a message flow diagram for the above-mentioned
20   relocation procedure.

DETAILED DESCRIPTION OF THE INVENTION

Figures 1, 2 described at the beginning of this document are schematic diagrams of network arrangements with interlinked network elements HLR/AuC, GGSN, old MSC/VLR,
25   old SGSN, new SGSN, new MSC/VLR: source (S)RNC, target (S)RNC, MS (mobile station), LA1 (LA2 = Location Update), LA2 RA1 (RA = Relocation Update), RA2. The reference symbol correspond to the abbreviations for mobile radio network elements normally used in mobile radio

technology. The broader lines show the connection from the mobile stations MS through the communication network. These same reference symbols/abbreviations are used in Figure 3. The message transmitted between the network elements are identified by numbers and abbreviations which are fixed expressions normally used in conjunction with mobile radio networks.

In Figure 3 the solution now makes provision, in an earlier phase of each relocation procedure to introduce at the new SGSN a buffering or intermediate storage of packets, regardless of whether the relevant subscriber is subject to surveillance or not, since this information is not yet available. Possible trigger points for the buffering of the data would be the messages "Forward Relocation Request" (3), "Relocation Request Acknowledge" (4) and "Relocation Detect" (9). The message actually used to trigger the buffering depends on the implementation, however the ready-to-store state should be established as early as possible.

The information as to whether surveillance is actually to be undertaken is not available until the end of the relocation procedure within the following RAU procedure (14) (RAU = Relocation Area Update) if the user data was transmitted. Up until that point all packets are buffered. If the subscriber is to be subject to surveillance his packets are not lost and can be further evaluated. If he is not to be subjected to surveillance, the packets are discarded. (after message block 14 in Figure 3) the average duration of the process amounts to appr. 5700 ms, for safety reasons the solution has been dimensioned so that a buffer time of 15 is retained to ensure that no data is lost even with delays.